PATENT ABSTRACTS OF JAPAN

(11)Publication number : **05-233459**

(43)Date of publication of application : **10.09.1993**

(51)Int.Cl. **G06F 12/14**

(21)Application number : **04-034936** (71)Applicant : **TOSHIBA CORP**

(22)Date of filing : **21.02.1992** (72)Inventor : **TOMOTA ICHIRO**

(54) **DATA BACKUP DEVICE**

(57)Abstract:

PURPOSE: To encipher and back up data which should be secret.

CONSTITUTION: Data used by an information processing system for a specific process are stored on a magnetic disk 1 and a protection deciding means 3 decides whether or not all access principal bodies have the right for read access to the data read out of the magnetic disk 1 according to access right information added to the data. When it is decided that at least one of the access principal bodies does not have the right for read access are enciphered by an enciphering part 4 and recorded on a magnetic tape 5, and when it is decided that all of the access principal bodies have the right for read access, the data are recorded on the magnetic tape 5 as they are.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] In the data backup equipment used for the information processing system equipped with the access protection feature The 1st storage which memorizes the data used for predetermined processing with said information processing system, A judgment means to judge whether an access subject reads to said data based on the access privilege information given beforehand about the data read from this 1st storage, and it has an access privilege, An encryption means to perform encryption about the data judged that at least one access subject reads with this judgment means, and do not have an access privilege, About the data judged that all access subjects read and have an access privilege from said judgment means, these data as it is It is data backup equipment

characterized by providing the 2nd storage which records and records the data enciphered with said encryption means about the data judged that said at least one access subject reads, and do not have an access privilege.

[Claim 2] The 2nd storage records the access privilege information beforehand given to these data with the data recorded. It judges with a judgment means whether based on the access privilege information given to these data to the data read from said 2nd storage, an access subject reads to said data, and it has an access privilege. At least one access subject reads with this judgment means, and a decryption is performed with a decryption means about the data judged that do not have an access privilege. About the data judged that all access subjects read and have an access privilege from said judgment means, these data Or it is data backup equipment according to claim 1 characterized by writing the data decrypted with said decryption means about the data judged that said at least one access subject reads, and do not have an access privilege in the 1st storage, respectively.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] this invention relates to the data backup equipment boiled and used for the information processing system equipped with the access protection feature.

[0002]

[Description of the Prior Art] Recently, although various kinds of information processing system is used, in such a system, data are sometimes plentifully destroyed owing to failure or a failure.

[0003] So, in the former, the data processed by the system are copied and saved

supposing such a situation, and when data are actually destroyed, the data backup equipment which restores the original data based on the saved data and which performs the so-called backup is used.

[0004] On the other hand, in information processing system, the access protection feature is prepared from ****** as what protects data from colander access in order to protect security and privacy generally.

[0005] The access protection feature in this case is constituted by the means for setting up access privilege information, and means to perform an access control. Access privilege information is the information about whether it has the right to which which access subject performs what kind of access to which data processed within a system here. Whether although an access subject accesses, he means things, and each access subject is considered by making what into a unit changes with systems. For example, the case where consider each user registered into the system to be each access subject, set up access privilege information in the form whether it has the right to which each user performs what kind of access to each data processed within a system, and access protection is performed can see. Moreover, what, in addition to this, considers each command in a system to be each access subject, and performs access protection, and the thing which considers each processor which constitutes a system to be each access subject, and realizes an access protection feature in hardware can also be seen. Moreover, an access-control means is judging whether it being what it should be permitted based on said access privilege information, and preventing access which should be permitted and which does not come out, when access tends to be performed by the access subject to data.

[0006]

[Problem(s) to be Solved by the Invention] However, when data were backed up in the information processing system equipped with such an access protection feature, the following troubles had occurred.

[0007] First, even if it can make access protection sufficient about the data which are in a processing process in information processing system, it is that it exists

mostly that it is difficult to perform access protection sufficient about what carried out copy preservation of it by backup. For example, generally, when backing up the file system on a magnetic disk with a magnetic tape, although a file system can perform access protection to the file on a magnetic disk, it may be unable to perform access protection even to the file on a magnetic tape.

[0008] In such a case, when suited on a magnetic disk, even if it is the file which restricted the user with the right read for security protection or privacy protection, about what recorded it by backup, that it will be in the condition in which read-out also to a user without the right originally read is possible arises. In addition, the medium of a magnetic tape etc. which can be renewed was used in many cases, and moreover, since these media were easy to carry, the medium for generally recording backup may have been stolen.

[0009] This invention was made in view of the above-mentioned situation, and aims at offering the data backup equipment which is stabilized and can secure security protection and privacy protection to the data saved by backup.

[0010]

[Means for Solving the Problem] In the data backup equipment with which this invention is used for the information processing system equipped with the access protection feature The 1st storage which memorizes the data used for predetermined processing with information processing system, A judgment means to judge whether an access subject reads to said data based on the access privilege information given beforehand about the data read from this 1st storage, and it has an access privilege, An encryption means to perform encryption about the data judged that at least one access subject reads with this judgment means, and do not have an access privilege, All access subjects read from a judgment means, and these data are recorded as it is about the data judged that have an access privilege. At least one access subject reads and it is constituted by the 2nd storage which records the data enciphered with said encryption means about the data judged that do not have an access privilege.

[0011] Moreover, the 2nd storage records the access privilege information

beforehand given to these data with the data recorded. It judges with a judgment means whether based on the access privilege information given to these data to the data read from the 2nd storage, all access subjects read to said data, and it has an access privilege. At least one access subject reads with this judgment means, and a decryption is performed with a decryption means about the data judged that do not have an access privilege. About the data judged that all access subjects read and have an access privilege from the judgment means, these data as it is Or said at least one access subject reads, and it is constituted so that the data decrypted with said decryption means about the data judged that do not have an access privilege may be written in the 1st storage, respectively.

[0012]

[Function] Consequently, about the data in which at least one access subject does not have a read-out access privilege according to this invention, it enciphers as data with the need for confidentiality, and backs up, and about the data in which all access subjects have a read-out access privilege, it comes to back up as it is, without enciphering as data without the need for confidentiality, and the security protection about backup data and privacy protection can be secured.

[0013]

[Example] Hereafter, one example of this invention is explained according to a drawing.

[0014] Drawing 1 shows the outline configuration of the operating system with which the data backup equipment of this example is applied. 1 is the magnetic disk which constitutes the file system whose storing of multiple files was enabled, and this magnetic disk 1 has write-in read-out of a file controlled by the disk control section 2 in drawing.

[0015] The protection judging section 3 is connected to the disk control section 2. It has connected also with the tape control section 6 mentioned later, and this protection judging section 3 judges whether based on the access privilege information beforehand set as these files, all access subjects have a read-out

access privilege to this file about the file content read from the file content read from the magnetic disk 1, or the magnetic tape 5 mentioned later, and performs read-out access protection. And he is trying to give the file content read from the file content read from the magnetic disk 1 based on the judgment result in this protection judging section 3, or the magnetic tape 5 mentioned later to a code and the decryption section 4 or the magnetic tape control section 5, and the disk control section 2. A well-known DES method etc. is used for a code and the decryption section 4, and file data enciphers or decrypts it.

[0016] 5 is the magnetic tape which stores two or more backup files, and this magnetic tape 5 has write-in read-out of a file controlled by the magnetic tape control section 6.

[0017] 7 is a control section, and this control section 7 performs each control of the disk control section 2, the protection judging section 3, a code and the decryption section 4, and the magnetic tape control section 6, and outputs a control command to each [these] circuit. Next, actuation of the example constituted as mentioned above is explained.

[0018] In this case, in the file system of the operating system used as the object which backs up by this example, three attributes, U, G, and P, are given as access privilege information about each file stored in a magnetic disk 1. And such an operating system is a system used by two or more users, and can define a user group now as a set of a user.

[0019] Here, the attribute U given to each file holds the identifier of a user with the ownership of a file. Moreover, an attribute G holds a user group's identifier to which the file belongs. Furthermore, an attribute P is 6 bits in binary-integer value which shows what kind of user has what kind of access privilege to the file. Whether the user who shows U attribute has the 0th bit of the right which reads the file Whether the user who shows U attribute has the 1st bit of the right written in the file Whether although it is not the user who shows U attribute, the user who belongs to the user group who shows G attribute has the 2nd bit of the right which reads the file Whether although it is not the user who shows U attribute,

the user who belongs to the user group who shows G attribute has the 3rd bit of the right written in the file The 4th bit is not [in addition] the user who shows U attribute, either. And whether the user who does not belong to the user group who shows G attribute, either has the right which reads the file It is shown whether the user who does not belong to the user group who is not the user who shows U attribute, either and shows G attribute, either has the 5th bit of the right written in the file (any bit shows having a right being shown and not having it at the time of 0, when the value is 1.). .

[0020] And the backup record in such an operating system stops operation of the magnetic disk 1 in a file system periodically, and is performed by copying the contents to a magnetic tape 6 about all the files that exist in a magnetic disk 1 between them. In this case, the command which records backup with an operating system is offered. From this condition, data logging for backup is performed according to the processing flow shown in drawing 2 with the command which directs backup. In this case, the file which is going to back up from a magnetic disk 1 is read by the disk control section 2 (step S21).

[0021] Next, the file which carried out in this way and was read is given to the protection judging section 3, and a read-out access protection judging is performed based on the attribute value of a file (step S22). In this case, the whole of the 0th of the P attribute of that file, the 2nd, and the 4th bit is judged by whether it is 1 whether all users have the right which reads the contents of the file. That is, if the 0th of P attribute, the 2nd, and the 4th bit are expressed as p0, p2, and p4, respectively, the reading appearance access protection judging result c will be calculated by c=p0^p2^p4. (^ means an AND)

[0022] And when the value of c is 1 as a judgment result here, it is judged that encryption of a file is unnecessary (step S23), and a file is given to the direct magnetic tape control section 6, and is written in a magnetic tape 5 (step S25).

[0023] On the other hand, when the value of c is 0 as a judgment result of the protection judging section 3, it is judged that encryption of a file is required (step S23), and a file is given to a code and the decryption section 4 (step S24). In a

code and the decryption section 4, it enciphers using a well-known DES method etc. about the file data judged that encryption is required. And the contents of this enciphered file are given to the magnetic tape control section 6, and come (step S25) to be written in a magnetic tape 5. In this case, each value of U attribute given to the file, G attribute, and P attribute also comes to be written in a tape. Hereafter, a backup process is performed about all the files similarly stored in the magnetic disk 1.

[0024] therefore, about the data in which at least one access subject does not have a read-out access privilege if it does in this way About the data in which it enciphers as data with the need for confidentiality, and it backs up and all access subjects have a read-out access privilege Since it can back up as it is, without enciphering as data without the need for confidentiality Efficient confidentiality can be acquired to the data saved by backup, the danger of infringing on the security and privacy to backup data is removed, it is stabilized and these security protection and privacy protection can be secured.

[0025] Next, the backup reconstitution of data which did in this way and was recorded on the magnetic tape 5 is performed according to the processing flow shown in drawing 3 with the command which directs restoration of backup.

[0026] In this case, the file which it is going to restore from a magnetic tape 5 is read by the magnetic tape control section 6 (step S31). In this case, each value of U attribute recorded on the magnetic tape 5, G attribute, and P attribute is also read in the case of the backup record mentioned above.

[0027] Next, the file which carried out in this way and was read is given to the protection judging section 3, and a read-out access protection judging is performed based on the attribute value of a file (step S32). In this case, based on the value of P attribute restored from the magnetic tape 5, it is carried out like the read-out access protection judging on the occasion of the record mentioned above. That is, if the 0th of P attribute restored from the magnetic tape 5, the 2nd, and the 4th bit are expressed as p0', p2', and p4', respectively, the read-out access protection judging result c will be calculated by c=p0"p2"p4'. (^ means an

AND)

[0028] And when the value of c is 1 as a judgment result here, it is judged that a decryption of a file is unnecessary (step S33), and a file is given to the direct disk control section 2, and is written in a magnetic disk 1 (step S35).

[0029] On the other hand, when the value of c is 0 as a judgment result of the protection judging section 3, it is judged that a decryption of a file is required (step S33), and a file is given to a code and the decryption section 4 (step S34). In a code and the decryption section 4, it decrypts about the file data judged that a decryption is required. And the contents of this decrypted file are given to the magnetic-disk control section 2, and come (step S35) to be written in a magnetic disk 1. Hereafter, all the files similarly stored in the magnetic tape 5 for backup will be restored to a magnetic disk 1.

[0030] therefore, about the data in which at least one access subject does not have a read-out access privilege about the backed-up data even if such About the data in which it decrypts as data with the need for confidentiality, and restores, and all access subjects have a read-out access privilege Since it can restore without decrypting as data without the need for confidentiality Also in the case of the reconstitution of data saved by backup, efficient confidentiality can be acquired to data, the danger of infringing on the security and privacy to the data restored can be removed, it is stabilized and these security protection and privacy protection can be secured. This invention can also be applied to backup of the contents of a communication link in an electronic mail system as other examples.

[0031] In this case, although there are two kinds of formats, a postcard format and a sealed letter format, in mail in an electronic mail system, and the mail of the postcard format of these is comparatively cheap, it is provided, the contents are restricted within a certain fixed magnitude and the confidentiality of the contents is not guaranteed, the mail of a sealed letter format is comparatively expensive, and it is provided, and the magnitude of the contents is not restricted but the confidentiality of the contents is guaranteed.

[0032] Then, about the mail of postcard form, read-out access by the transmitting person of the mail, write-in access, and read-out access by all users are permitted, and only read-out access by the transmitting person of the mail, write-in access, and read-out access by the addressee of e-mail are permitted [mail / of sealed letter form]. That is, be made to let it be access privilege information whether for the form of e-mail to be either a postcard or a sealed letter.

[0033] When the backup in this e-mail system has the Request to Send of e-mail by the user using two floppy disk drive units F0 and F1, the mail of postcard form has realized mail of sealed letter form by recording the contents of e-mail F1 to F0 again.

[0034] In this case, as shown in the flow chart of drawing 4 , a read-out access protection judging is performed first (step S41). a ****** [that read-out to all users is possible for the contents of e-mail here] -- ** -- a ****** [that the mail of saying is postcard form] -- ** -- since it is equivalent to saying, it investigates what the form of the mail used as the candidate for backup is as a read-out access protection judging.

[0035] And if it judges with the mail of a postcard format as a judgment result here (step S42), it will record on F0, without enciphering the contents (step S43). On the other hand, if it judges with the mail of a sealed letter format at step S42, the contents of e-mail will be enciphered (step S44), and it will come (step S45) to record on F1.

[0036] Therefore, also in an electronic mail system, as mentioned above, efficient confidentiality can be acquired to the mail saved by backup like the case where it backs up, the danger of infringing on the security and privacy to backup mail is removed, it is stabilized and these security protection and privacy protection can be secured. In addition, this invention is not limited only to the above-mentioned example, but in the range which does not change a summary, deforms suitably and can be carried out.

[0037]

[Effect of the Invention] According to this invention, the security of the data which

lead backup about the required data of confidentiality in backup of data, and the danger of infringement of privacy are eliminated, it is stabilized and security protection and privacy protection can be secured. Moreover, backup of data can be realized efficiently, without needing count of unnecessary encryption and decryption, since it is made to back up only by performing encryption and a decryption about the required data of confidentiality.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing showing the outline configuration of one example of this invention.

[Drawing 2] The flow chart for explaining actuation of the example of drawing 1 .

[Drawing 3] The flow chart for explaining actuation of the example of drawing 1 .

[Drawing 4] The flow chart for explaining other examples of this invention.

[Description of Notations]

1 [-- A code and the decryption section, 5 / -- A magnetic tape, 6 / -- A tape control section, 7 / -- Control section.] -- A magnetic disk, 2 -- A disk control section, 3 -- The protection judging section, 4